

WHAT IS CLAIMED IS:

1           1. A system for delivering content to a subscriber terminal on-demand  
2 through a communication network, the system comprising:  
3               a content preparation module for preencrypting the content offline to form pre-  
4 encrypted content;

5               an on-demand module receiving the pre-encrypted content from the content  
6 preparation module, for storing, and transmitting the pre-encrypted content to the subscriber  
7 terminal when authorized;

8               an encryption renewal system interfacing with the on-demand module to  
9 generate entitlement control messages allowing the pre-encrypted content to be decryptable  
10 for a designated duration; and

11               a conditional access system for providing a periodical key to the encryption  
12 renewal system, to permit generation of the entitlement control messages that convey  
13 information required to decrypt the pre-encrypted content including the periodical key to the  
14 subscriber terminal.

1           2. The system of claim 1 wherein the communication network is a cable  
2 network for distributing audio/video content from a cable central office to all or a subset of  
3 subscriber terminals.

1           3. A method of delivering content from one or more cable systems to  
2 subscriber terminals within the cable systems, the cable systems being communicatively  
3 coupled to an offline encryption device, the method comprising:

4               receiving by a first cable system, a request for the content from a first  
5 subscriber terminal of the first cable system;

6               preencrypting, by the offline encryption device, the content to form pre-  
7 encrypted content prior to the step of receiving a request;

8               generating an encryption record containing parameters employed for  
9 encrypting the content;

10               based on the encryption record and a first key information, generating one or  
11 more control messages for permitting access to the pre-encrypted content; and

12               transmitting the pre-encrypted content associated with the one or more control  
13 messages to the first subscriber terminal for decryption of the pre-encrypted content.

1                   4.       The method of claim 3 further comprising  
2                   receiving, by a second cable system, a request from a second subscriber  
3                   terminal of the second cable system, and  
4                   based on the encryption record and a second key information, generating one  
5                   or more control messages for permitting the second subscriber terminal to access the pre-  
6                   encrypted content.

1                   5.       The method of claim 3 wherein the first key information is provided by  
2                   a conditional access system that uses the key information to control the first subscriber  
3                   terminal.

1                   6.       The method of claim 5 wherein the key information is for a key that is  
2                   periodical and valid for a designated duration.

1                   7.       The method of claim 6 wherein the designated duration is shortly  
2                   before, contemporaneous with, or shortly after the first key is changed by the conditional  
3                   access system.

1                   8.       The method of claim 3 wherein the one or more control messages is a  
2                   first entitlement control message for conveying information to the first subscriber terminal to  
3                   compute a key.

1                   9.       The method of claim 3 further comprising  
2                   changing the first key information after a designated duration, and reporting  
3                   the key change by the first cable system.

1                   10.      The method of claim 3 further comprising  
2                   retrofitting a second entitlement control message to the pre-encrypted content  
3                   for permitting access to the pre-encrypted content after the first key information expires.

1                   11.      The method of claim 10 wherein the retrofitting of the second control  
2                   message employs a second key information.

1                   12.      The method of claim 11 wherein the step of retrofitting the second  
2                   entitlement control message is synchronized with changing of a first key information to the  
3                   second key information.

1                   13.     The method of claim 3 further comprising  
2                   providing the parameters from an encryption renewal system that generates the  
3                   one or more entitlement control messages.

1                   14.     The method of claim 13 wherein the step of generating an encryption  
2                   record is by an offline encryption system.

1                   15.     The method of claim 4 further comprising  
2                   providing first and second service tiers in the first cable system to further limit  
3                   access to the pre-encrypted content.

1                   16.     The method of claim 15 further comprising  
2                   generating a first entitlement control message allowing the first subscriber  
3                   terminal to access the pre-encrypted content only in the first service tier, and  
4                   generating a second entitlement message allowing a second subscriber  
5                   terminal to access the pre-encrypted only in the second service tier.

1                   17.     A system for delivering first and second content to a subscriber  
2                   terminal on-demand through a communication network, the system comprising:  
3                   means for pre-encrypting the first and second content offline to form first and  
4                   second pre-encrypted content, and for generating a first encryption record associated with the  
5                   first pre-encrypted content, and a second encryption record for the second pre-encrypted  
6                   content;  
7                   means for generating a first and second entitlement messages that allow  
8                   decryption of the first and second pre-encrypted contents, respectively;  
9                   a conditional access system for providing information included in the first and  
10                  second entitlement messages by the means for generating; and  
11                  means for receiving the pre-encrypted content from the means for pre-  
12                  encrypting, forwarding the first and second encryption records to the means for generating  
13                  which generates the first and second entitlement messages for forwarding to the subscriber  
14                  terminal.  
1                   18.     The system of claim 17 further comprising means for generating a  
2                   third entitlement message.

1                   19.    The system of claim 18 wherein the third entitlement message is for  
2 permitting access to the first pre-encrypted content after expiration of the first entitlement  
3 message.

1                   20.    A method using an encryption renewal system, the method permitting  
2 first and second communication systems to control subscriber access to pre-encrypted content  
3 that was previously encrypted offline, the method comprising:

4                   receiving, by the encryption renewal system, a first cryptographic information  
5 from the first communication system;

6                   receiving an encryption record containing parameters employed during  
7 encryption to form the pre-encrypted content; and

8                   generating for the first communication system, a first control message for  
9 providing access to the pre-encrypted content based on the first cryptographic information  
10 and the first encryption record.

11                  21.    The method of claim 20 further comprising

12                  receiving, by the encryption renewal system, a second cryptographic  
13 information from the second communication system;

14                  receiving the encryption record containing parameters employed during  
15 encryption to form the pre-encrypted content; and

16                  generating for the second communication system, a second control message  
17 for providing access to the pre-encrypted content based on the second cryptographic  
18 information and the encryption record.

1                   22.    The method of claim 20 further comprising generating a third control  
2 message upon expiration of the first control message, to provide access to the pre-encrypted  
3 content.

1                   23.    The method of claim 20 further comprising

2                  retrieving entitlement control messages associated with the pre-encrypted  
3 content; and

4                  specifying a tier to which a subscriber is authorized when the pre-encrypted  
5 program is purchased.

1                   24. A system for delivering content to a subscriber terminal on-demand  
2 through a point-to-point communication network, the system comprising:  
3                   an offline encryption system having software containing one or more  
4 instructions for pre-encrypting the content to form pre-encrypted content before a content  
5 request is received from the subscriber terminal;  
6                   a video on-demand system including software having one or more instructions  
7 for receiving the pre-encrypted content from the offline encryption system, and forwarding  
8 the pre-encrypted content to the subscriber terminal; and  
9                   an encryption renewal system interfacing with the offline encryption system to  
10 provide encryption parameters for encrypting the content, and interfacing with the video on-  
11 demand system to generate entitlement control messages allowing the pre-encrypted content  
12 to be decryptable for a designated duration, wherein the entitlement control messages are  
13 generated by using a periodical key.

1                   25. The system of claim 24 further comprising a conditional access system  
2 having software interfacing with a billing system to coordinate subscriber access to the pre-  
3 encrypted content based on a subscriber purchase.

1                   26. The system of claim 24 further comprising an interactive system  
2 including software having instructions for providing two-way subscriber interaction between  
3 the subscriber system and the video on-demand system.

1                   27. The system of claim 24 further comprising one or more service tiers to  
2 secure the pre-encrypted content.

1                   28. The system of claim 24 wherein the encryption renewal system  
2 generates first and second versions of an entitlement control message, for accessing the pre-  
3 encrypted content in a first and a second tier, respectively.

1                   29. The system of claim 24 further comprising  
2 retrieving entitlement control messages associated with the pre-encrypted  
3 content, and specifying the tier for which a subscriber is authorized when the pre-encrypted  
4 program is purchased.

1                   30.    The system of claim 24 wherein the encryption renewal system  
2 provides a call back mechanism indicating the next time by which the video on-demand  
3 system should contact the encryption renewal system.

1                   31.    The method of claim 20 further comprising providing a call back  
2 mechanism.

1                   32.    The method of claim 20 further comprising maintaining a list of first,  
2 second and third communication systems and their addressing information.

1                   33.    The method of claim 3 wherein the step of pre-encrypting is carried out  
2 using a third key, and the encryption record contains information about the third key.

1                   34 .    The method of claim 33 further comprising translating the third key  
2 into the first key information.

1                   35.    The system of claim 25 wherein the video on-demand system and the  
2 conditional access system are decoupled.

1                   36.    The system of claim 25 wherein the video on-demand system and the  
2 conditional access systems comprise a first cable system, each communicably coupled to the  
3 encryption renewal system.

1                   37.    The system of claim 36 further comprising a second cable system  
2 having a second conditional access system and a second video on-demand system each  
3 communicably coupled to the encryption renewal system.

1                   38.    A method of delivering pre-encrypted content to subscribers from a  
2 first and a second communication system the method comprising:

3                    preencrypting the content once at a centralized facility, and prior to  
4 distribution to the first and second communication systems;

5                    if the first communication is authorized to receive the content, transmitting the  
6 content to the first communication system;

7                    storing the content by the first communication system;

8                    if the second communication system is authorized to receive the content,  
9 transmitting the content to the second communication system; and

1 40. The method of claim 20 further comprising assigning subscriber tiers,  
2 so that only a designated number of subscribers share each subscriber tier within a fiber node.